PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-281003
(43)Date of publication of application : 03.10.2003

(51)Int.Cl. G06F 13/00
H04L 12/66

(21)Application number : 2002-087392
(22)Date of filing : 27.03.2002

(71)Applicant : HITACHI LTD
(72)Inventor : TERADA MASATOSHI
ISOGAWA HIROMI
OSADA KIYOTO

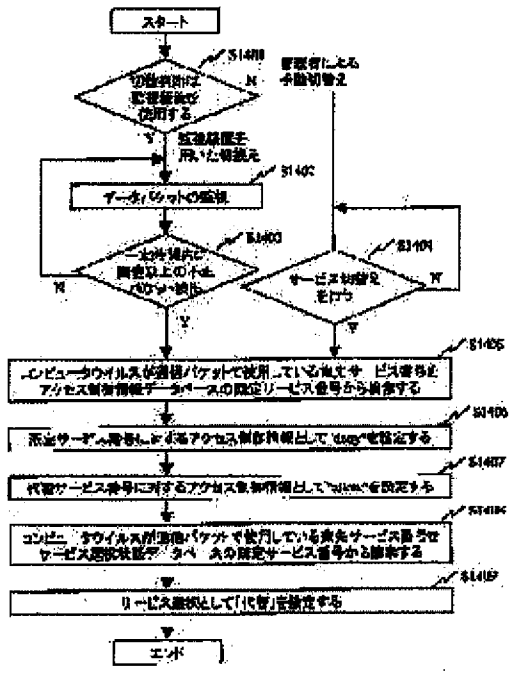
(54) SUPPORT METHOD FOR GUARANTEEING OPERATION OF SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To guarantee the operating property of communication or the like in a network system by suppressing the spreading of a computer virus even though no virus-disinfection tool is distributed.

SOLUTION: When a computer virus spreads, 'pass rejection' is stored in access control information 53 for a destination service number 1002 used by the computer virus in a communication packet as switching of access control of a pass service (S1406), and 'pass permission' is stored in access control information 55 for a substitute service number 54 (S1407). Thereby, the communication packet of the computer virus is interrupted and the communication packet of the substitute service number is filtered out. 'Substitute' showing selection of the substitute service number as a service number used by a normal application program is stored in service selection 74 as a switching operation to a substitute service (S1409). By doing this, a substitute service number 73 subjected to the 'pass permission' is thereafter used to perform communication.

図 14



(Partial Translation)
JP 2003-281003 A

[0006]
[Means for solving problem] The present invention is achieved by the means explained below as a support method for guaranteeing system operation for a network system that is configured with equal to or more than one device using an electronic calculator for solving the above problem.

(1) Detecting abnormal traffic
Traffic generated by a computer virus such as a worm is detected. Traffic is identified when a traffic pattern that differs from a normal mode is generated exceeding a threshold value or from initial analytical information concerning a computer virus.

(2) Switching destination service number
A destination service number used by the traffic that is detected at the first step is switched to a substitute service number that is used when a computer virus spreads.

(3) Switching access control of pass service
Traffic with the substitute service number selected at the second step is only allowed to pass and traffic with the destination service number detected at the first step is blocked.

[0007] Even if a computer virus such as a worm spreads in a targeted network system, these means allows suppressing such spreading and ensuring operability of the system.

[0008] According to the support for guaranteeing system operation of the present invention, only switching the support apparatus for guaranteeing system operation to a substitute service mode enables blocking the traffic

related to a computer virus such as a worm and allows passing only the traffic used by an authorized application. Accordingly, even if a disinfection tool against a computer virus is not distributed, spreading of the computer virus can be suppressed, and operability of the communication in a network system can be ensured.

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2003－281003
（P2003－281003A）
(43)公開日　平成15年10月3日(2003.10.3)

(51)Int.Cl.[7]	識別記号	Ｆ Ｉ	テーマコード(参考)
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｚ　５Ｂ０８９
Ｈ０４Ｌ　12/66		Ｈ０４Ｌ　12/66	Ｂ　５Ｋ０３０

審査請求　未請求　請求項の数６　ＯＬ　（全 18 頁）

(21)出願番号　特願2002－87392(P2002－87392)

(22)出願日　平成14年３月27日(2002.3.27)

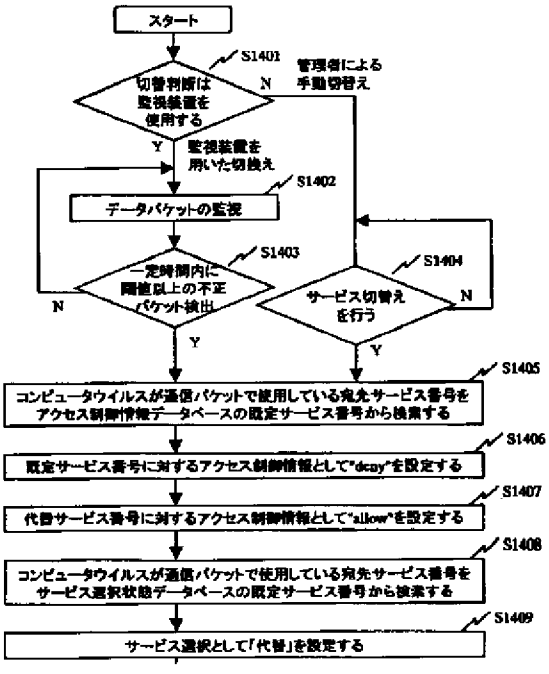
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　寺田　真敏
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　磯川　弘実
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　システム稼動保証支援方法

(57)【要約】
【課題】駆除ツールが配布されていなくともコンピュータウイルスの拡散を抑止し、ネットワークシステムにおける通信などの稼動性を保証する。
【解決手段】コンピュータウイルスの拡散時、通過サービスのアクセス制御の切替えとして、コンピュータウイルスが通信パケットで使用している宛先サービス番号1002に対するアクセス制御情報53に「通過拒否」を格納し(S1406)、代替サービス番号54に対するアクセス制御情報55に「通過許可」を格納することにより(S1407)、コンピュータウイルスの通信パケットを遮断し、代替サービス番号の通信パケットを透過させる。代替サービスへの切替え操作として、正規のアプリケーションプログラムが使用するサービス番号として、サービス選択74に代替サービス番号の選択を示す「代替」を格納することにより(S1409)、以降、「通過許可」された代替サービス番号73を使用して通信を行う。

図 14



1

【特許請求の範囲】
【請求項１】ネットワークに接続した電子計算機から成るシステムにおいて、コンピュータウイルス拡散中ではない状態で使用する既定サービス番号を設け、コンピュータウイルス拡散中には既定サービス番号に対するアクセス制御によりトラフィックを止めることを特徴とするシステム稼動保証支援方法。
【請求項２】請求項1記載のシステム稼動保証支援方法において、コンピュータウイルス拡散中に使用する代替サービス番号を設け、コンピュータウイルス拡散中には代替サービス番号に対するアクセス制御によりトラフィックを通過させ、コンピュータウイルス拡散中には代替サービス番号を用いて通信を行うことを特徴とするシステム稼動保証支援方法。
【請求項３】請求項1記載のシステム稼動保証支援方法において、不正パケット監視によるコンピュータウイルスの流布を検知することを特徴とするシステム稼動保証支援方法。
【請求項４】請求項2記載のシステム稼動保証支援方法において、既定サービス番号と代替サービス番号との対応付けデータベースを検索し、既定サービス番号から代替サービス番号に切替えることを特徴とするシステム稼動保証支援方法。
【請求項５】請求項2記載のシステム稼動保証支援方法において、事前に登録されたプログラムのみが代替サービス番号を用いた通信を行えるように設定し、特定の宛先アドレスに対してのみ代替サービス番号を用いた通信を行えるようにすることを特徴とするシステム稼動保証支援方法。
【請求項６】請求項2記載のシステム稼動保証支援方法において、特定のURLを書換えることを特徴とするシステム稼動保証支援方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワークに接続した電子計算機から成るシステムに対し、コンピュータウイルスの拡散を抑止し、さらに、当該ネットワークシステムにおける通信などの稼動性を保証する技術に関する。
【０００２】
【従来の技術】近年、企業情報システムにおけるワームなどのコンピュータウイルス流布対策は重要な課題となってきている。従来、ワームなどのコンピュータウイルス流布を予防するため、各社から提供されているウイルス対策ソフトウェアを用いることにより、コンピュータウイルスの検出、駆除ならびに、感染からの修復などが行われている。
【０００３】
【発明が解決しようとする課題】インターネット技術な

2

れるにつれ、ワームなどのコンピュータウイルスが流布した際にも定常的に稼動することのできるネットワークシステムが求められている。
【０００４】しかしながら、上記従来技術を用いてコンピュータウイルスの流布対策を行う場合、該当するコンピュータウイルスの駆除ツールを適用することで流布を抑止するため、駆除ツールが配布され、さらに適用されない限りコンピュータウイルスの拡散を抑止することができない。また、すべてのシステムでの対策が完了しないとコンピュータウイルスの拡散に付随して発生するトラフィック増加を抑止できず、結果としてコンピュータウイルスの影響を受けないシステムも利用することができないなど、ネットワークシステム全体の稼動性を保証することができないという課題がある。
【０００５】本発明では上記問題点の解決を図り、コンピュータウイルスの駆除ツールが配布されていなくともコンピュータウイルスの拡散を抑止し、さらに、当該ネットワークシステムにおける通信などの稼動性を保証することを目的とする。
【０００６】
【課題を解決するための手段】本発明は、上記課題を解決するために、電子計算機を用いて1以上の機器で構成されるネットワークシステムにシステム稼動保証支援方法として、以下に示す手段を用いることにより達成される。
(1) 異常トラフィックの検知
ワームなどのコンピュータウイルスが生成するトラフィックを検知する。通常状態とは異なるトラフィックパターンが閾値以上に発生した場合や、コンピュータウイルスに関する初期解析情報からトラフィックを特定する。
(2) 宛先サービス番号の切替え
前記第1ステップにより検知したトラフィックが使用している宛先サービス番号を、コンピュータウイルスが流布した際に使用する代替サービス番号に切り替える。
(3) 通過サービスのアクセス制御の切替え
前記第2ステップにより選択した代替サービス番号のトラフィックのみを通過させ、前記第1ステップにより検知した宛先サービス番号のトラフィックを止める。
【０００７】これらの手段により、対象とするネットワークシステムにおいてワームなどのコンピュータウイルスが拡散した際にも、その拡散の抑止すると共に、システムの稼動性を確保することができる。
【０００８】本発明のシステム稼動保証支援によれば、システム稼動保証支援装置を代替サービス状態に切り替えるだけで、ワームなどのコンピュータウイルスに関わるトラフィックを止め、かつ、正規のアプリケーションプログラムが使用するトラフィックのみを通過させるので、コンピュータウイルスの駆除ツールが配布されていなくともコンピュータウイルスの拡散を抑止し、さら

確保することができる。

【０００９】

【発明の実施の形態】以下、本発明の第1実施例を図面によって説明する。

【００１０】図3は、本実施例を適用したシステム稼動保証支援のネットワークシステム概略図である。システム稼動保証支援装置31a，31b、そして、サーバ装置32a、クライアント装置32bなどの電子計算機がネットワーク33aを介して接続している。なお、システム稼動保証支援装置31bはサーバ装置機構をその装置内部に取り込んだ構成となっている。

【００１１】図1は、システム稼動保証支援装置31の概略構成図である。システム稼動保証支援装置31は、CPU11、メモリ12、ハードディスク装置などの外部記憶装置13、ネットワークに接続された通信装置14、キーボードやマウスなどの入力装置15、ディスプレイなどの表示装置16、FDなどの可搬性を有する記憶媒体のデータにアクセス読取り装置17と、上述した各構成要素間のデータ送受信を司るインタフェース18とを備えた電子計算機上に構築することができる。外部記憶装置13には、システム稼動保証支援装置31を電子計算機上に構築するための構成情報管理プログラム133、当該装置上で稼動するアプリケーションプログラム136などが格納されている。

【００１２】CPU11はメモリ上にロードされた構成情報管理プログラム133を実行することにより、稼動保証支援装置全体のプロセス制御を行う。不正パケット監視部112は不正パケットのパターン情報が格納されたデータベース131に合致するパケットを検出する。入力制御部111は入力装置15や表示装置16を制御して稼動保障支援装置の管理者から指示を受け付けたりその出力を表示したりする。構成情報管理プログラム133は、これらパケット監視部112と入力制御部111と連動して、コンピュータウイルスの拡散時には、システムの構成情報が格納されたデータベース134からコンピュータウイルスの拡散時に使用する構成情報を抽出し、データ転送プログラム132に構成情報を設定することによりコンピュータウイルスの拡散を抑止するようトラフィックの制御を行う。

【００１３】図2は、クライアント装置やサーバ装置などのネットワークシステムを利用する電子計算機32の概略構成図である。ここで、図1に示すシステム稼動保証支援装置31と同じ機能を有するものには同じ符号を付している。クライアント／サーバ装置32の外部記憶装置13には、当該装置上で稼動するアプリケーションプログラム136と、構成情報管理プログラム133が格納されている。CPU11はメモリ上にロードされた構成情報管理プログラム133を実行することにより、クライアント／サーバ装置全体のプロセス制御を行い、そのプロセス制御下でアプリケーションプログラム136を実行することにより、サーバ装置32aが有する個々のサービスを提供す

【００１４】図10は、本実施例のネットワークシステムで使用する通信用パケットの一例であり、クライアント装置32bからサーバ装置32aに送信する際に使用するパケットフォーマットである。列1001は宛先アドレスでサーバ装置32aのネットワーク上の論理アドレス、列1003は発信元アドレスでクライアント装置32bのネットワーク上の論理アドレスが格納される。列1002は宛先サービス番号でサーバ装置32a上のサーバアプリケーションプログラムが提供するサービスを一意に識別する番号、列1004は発信元サービス番号でクライアント装置32b上のクライアントアプリケーションプログラムのサービスを一意に識別する番号が格納される。

【００１５】図5～図6に、システム稼動保証支援装置31a，31bで使用する通過サービスのアクセス制御情報に関する構成情報データベース134の一例を示す。

【００１６】図5は、コンピュータウイルスが拡散中ではない状態の通過サービスのアクセス制御情報が格納されたデータベースである。列51aにはサーバアプリケーションプログラムのサービスを一意に識別する名称、列52aには同じ行のサービス名がコンピュータウイルス拡散中ではない状態で使用するサービスの識別番号が格納され、列53aには同じ行のサービス名が使用する既定サービス番号に対するアクセス制御情報であり、コンピュータウイルス拡散中ではないため「通過許可」を示す「allow」が格納される。これは、宛先サービス番号1002に値「80」が格納された通信パケットの通過を許可することを意味する。列54aには同じ行のサービス名がコンピュータウイルス拡散中に使用するサービスの識別番号、列55aには同じ行のサービス名が使用する代替サービス番号に対するアクセス制御情報であり、コンピュータウイルス拡散中ではないため「通過拒否」を示す「deny」が格納される。これは、宛先サービス番号1002に値「9080」が格納された通信パケットの通過を拒否することを意味する。

【００１７】図6は、サービス名httpに関わるトラフィックを利用してコンピュータウイルスが拡散している際の通過サービスのアクセス制御情報が格納されたデータベースであり、図6の各列は図5に示す各列に対応している。列53bには同じ行のサービス名が使用する既定サービス番号に対するアクセス制御情報である。サービス名httpに関わるトラフィックを利用してコンピュータウイルスが拡散していることから、httpが使用する既定サービス番号52bに対するアクセス制御は「通過拒否」を示す「deny」が格納され、それ以外の既定サービス番号52bに対するアクセス制御は「通過許可」を示す「allow」が格納される。

【００１８】列55bには同じ行のサービス名が使用する代替サービス番号54bに対するアクセス制御情報であり、httpに関わるトラフィックを利用してコンピュータ

サービス番号54bに対するアクセス制御は「通過許可」を示す「allow」が格納され、それ以外の代替サービス番号54bに対するアクセス制御は「通過拒否」を示す「deny」が格納される。これは、コンピュータウイルスが送信する宛先サービス番号1002に値「80」を格納した通信パケットを遮断し、それ以外のアプリケーションプログラムによる通信パケットを通過させることを意味する。

【００１９】図7に、システム稼動保証支援装置31a，31bならびにクライアント／サーバ装置32a，32bで使用するサービス選択状態に関する構成情報データベース134の一例を示す。図7は、サービス名httpに関わるトラフィックを利用してコンピュータウイルスが拡散している際のアプリケーションプログラムが使用するサービス番号とサービス選択状態が格納されたデータベースである。

【００２０】列71にはサーバアプリケーションプログラムのサービス名を一意に識別する名称、列72には同じ行のサービス名がコンピュータウイルス拡散中ではない状態で使用するサービス番号、列73には同じ行のサービス名がコンピュータウイルス拡散中に使用する代替サービス番号、列74には同じ行のサービス名が使用するサービス選択状態が格納され、サービス名httpに関わるトラフィックを利用してコンピュータウイルスが拡散していることから、サービス名httpではサービス選択状態値として「代替」、それ以外のサービス名ではサービス選択状態値として「既定」が格納される。

【００２１】ここで選択されたサービス選択値74に対応するサービス番号が通信パケットの宛先サービス番号1002に格納されるため、本実施例のネットワークシステムでは、正規のアプリケーションプログラムはサービス名httpについては宛先サービス番号1002として代替サービス番号「9080」を使用し、その他のサービスのひとつであるhttpsでは宛先サービス番号1002として既定サービス番号「443」を使用する。しかし、コンピュータウイルスには構成変更情報を提供しないので、コンピュータウイルスはサービス名httpについては通信パケットの宛先サービス番号1002として値「80」を使用し続けることになる。

【００２２】上記構成のシステム稼動保証支援装置31a，31bの動作について説明する。

【００２３】図14は、コンピュータウイルス拡散時のシステム稼動保証支援装置31a，31bの動作を説明するためのフロー図である。コンピュータウイルスの拡散に伴い、その拡散を抑止するためのサービス状態の切替えを不正パケット監視部112を用いて行うか、管理者の判断により行うかを判断する(ステップS1401)。

【００２４】不正パケット監視部112を用いてコンピュータウイルスの拡散を検知する場合、データパケットのパターンデータベース131に登録されているパターンに類似する不正パケットを一定時間内に閾値以上検出するとコンピュータウイルスが拡散中であると判断し(ステップS1403)、通過サービスのアクセス制御の切替え(ステップS1405～S1407)と代替サービスへの切替え(S1408～S1409)を行う。

【００２５】通過サービスのアクセス制御の切替え操作として、コンピュータウイルスが通信パケットで使用している宛先サービス番号1002を通過サービスのアクセス制御情報データベースの既定サービス番号52から探索し(ステップS1405)、探索結果に合致する該当行の既定サービス番号52に対するアクセス制御情報53に「通過拒否」を示す「deny」を格納し(ステップS1406)、代替サービス番号54に対するアクセス制御情報55に「通過許可」を示す「allow」を格納する(ステップS1407)。これにより、クライアント装置32b、サーバ装置32aの間に位置するシステム稼動保証支援装置31a，31bは、コンピュータウイルスが宛先サービス番号1002に既定サービス番号を設定している通信パケットを遮断し、宛先サービス番号1002にその代替サービス番号を設定している通信パケットのみを通過させる。

【００２６】次に、代替サービスへの切替え操作として、コンピュータウイルスが通信パケットで使用している宛先サービス番号1002をサービス選択状態データベースの既定サービス番号72から探索し(ステップS1408)、探索結果に合致する該当行のサービス選択74に代替サービス番号の選択を示す「代替」を格納する(ステップS1409)。

【００２７】一方、ステップS1401において、管理者の判断により行うを選択した場合、管理者が手動で切替えを行うことになる(S1405)。

【００２８】図15は、コンピュータウイルス拡散収束時のシステム稼動保証支援装置31a，31bの動作を説明するためのフロー図である。

【００２９】コンピュータウイルスの収束に伴い、サービス状態を通常状態に復帰するためのサービス状態の切替えを不正パケット監視部112を用いて行うか、管理者の判断により行うかを判断する(ステップS1501)。

【００３０】不正パケット監視部112を用いてコンピュータウイルスの収束を検知する場合、データパケットの監視を行い(ステップS1502)、不正パケットパターンデータベース131に登録されているパターンに類似する不正パケットを一定時間内に閾値以上検出しなくなった時点で収束と判断し(ステップS1503)、通過サービスのアクセス制御の復帰(ステップS1505)と既定サービスへの切替え(S1506)を行う。通過サービスのアクセス制御の復帰操作として、既定サービス番号52に対するアクセス制御情報53に「通過許可」を示す「allow」を格納し、代替サービス番号54に対するアクセス制御情報55に「通

スへの切替え操作として、サービス選択74として既定サービス番号の選択を示す「既定」を格納する。一方、ステップS1501において、管理者の判断により行うことを選択した場合、管理者が手動で切替えを行うことになる(S1504)。

【００３１】上記構成のクライアント／サーバ装置32a，32bの動作について説明する。

【００３２】図16は、コンピュータウイルス拡散時のクライアント／サーバ装置32a，32bの動作を説明するためのフロー図である。コンピュータウイルスの拡散に伴い、その拡散を抑止するためのサービス状態の切替えをシステム稼動保証支援装置31a,31bからの通知を用いて行うか、ユーザの判断により行うかを判断する(ステップS1601)。

【００３３】システム稼動保証支援装置31a，31bからの通知を用いてサービス状態の切替えを行う場合、切替え通知メッセージの監視を行い(ステップS1602)、切替え通知メッセージを受信すると代替サービスへの切替え(S1604～S1605)を行う。代替サービスへの切替えでは、コンピュータウイルスが通信パケットで使用している宛先サービス番号1002をサービス選択状態データベースの既定サービス番号72から探索し(ステップS1604)、探索結果に合致する該当行のサービス選択74として代替サービス番号の選択を示す「代替」を格納する(ステップS1605)。

【００３４】代替サービスへの切替え操作が終了すると、それ以降正規のアプリケーションプログラムのサービスを利用する場合には、通信パケットの宛先サービス番号1002に既定サービス番号72ではなく、システム稼動保証支援装置31a，31bのステップS1407において、アクセス制御情報55として「通過許可」された代替サービス番号73を設定して通信を行う。

【００３５】本実施例によれば、以下のような効果がある。

(1) システム稼動保証支援のサービス状態をコンピュータウイルスの拡散を抑止する状態へと切替えると、コンピュータウイルスが使用する通信パケットを遮断する。このため、当該コンピュータウイルスの拡散を抑止することができる。

(2) システム稼動保証支援のサービス状態をコンピュータウイルスの拡散を抑止する状態に切替えた際には、正規のアプリケーションプログラムは代替サービス番号を使用して通信を行う。このため、コンピュータウイルスが使用する通信パケットを遮断し、かつ正規のアプリケーションプログラムの通信サービスを保証することができる。

(3) システム稼動保証支援のサービス状態の切替えに侵入検知システムなどの不正パケット監視機能と連動させている。このため、サービス状態の自動切換えが実現で能となる。

【００３６】以下、本発明の第2実施例を図面によって説明する。第2実施例は、特定のアプリケーションプログラムのみが代替サービスに切替えることができることを示す実施例である。

【００３７】図3のネットワークシステム概略図、図1のシステム稼動保証支援装置31の概略構成図、図2の電子計算機32の概略構成図、図10の通信用パケットのフォーマット、図5～図6のシステム稼動保証支援装置31a，31bで使用する通過サービスのアクセス制御情報に関するデータベース、図14～図15のコンピュータウイルス拡散時ならびに収束時の動作を説明するためのフロー図は、第1実施例と同じである。

【００３８】図8～図9に、システム稼動保証支援装置31a，31bならびにクライアント／サーバ装置32a，32bで使用する構成情報データベース134の一例を示す。

【００３９】図8は、システム稼動保証支援機構を利用することのできるアプリケーションが登録されたデータベースである。列81には本実施例のシステム稼動保証支援機構を利用することのできるアプリケーションプログラムを一意に識別する名称が格納されている。

【００４０】図9は、サーバ毎にアプリケーションプログラムが使用するサービス番号とサービス選択状態が格納されたデータベースであり、testservサーバ32aに対してサービス名httpに関わるトラフィックを利用してコンピュータウイルスが拡散している際の設定となっている。列91aにはサーバを一意に識別するネットワーク上の論理アドレス、列92aにはサーバアプリケーションプログラムのサービス名を一意に識別する名称、列93aには同じ行のサービス名がコンピュータウイルス拡散中ではない状態で使用するサービス番号、列94aには同じ行のサービス名がコンピュータウイルス拡散中に使用する代替サービス番号、列95aには同じ行のサービス名が使用するサービス選択状態が格納される。

【００４１】testservサーバ32aに対してサービス名httpに関わるトラフィックを利用してコンピュータウイルスが拡散していることから、testservサーバ32aのサービス名httpではサービス選択状態値として「代替」、それ以外のサーバとサービス名ではサービス選択状態値として「既定」が格納される。ここで選択されたサービス選択値74に対応するサービス番号が通信パケットの宛先サービス番号1002に格納され、また、testservサーバ32aのネットワーク上の論理アドレスが宛先アドレス1001に格納されるため、本実施例のネットワークシステムでは、testservサーバ32aのサービス名httpについては宛先サービス番号1002として代替サービス番号「9080」を使用し、その他のサーバのサービス名httpでは宛先サービス番号1002として既定サービス番号「80」を使用する。なお、コンピュータウイルスには構成変更情報を

バ32aのサービス名httpについては通信パケットの宛先サービス番号1002として値「80」を使用し続けることになる。本実施例ではサービス名としてhttpを取り上げているが、電子メール、ファイル転送など他のサービス名についても同様に処理を行うことができる。

【００４２】上記構成のクライアント／サーバ装置32a，32bの動作について説明する。

【００４３】図17は、コンピュータウイルス拡散時のクライアント／サーバ装置32a，32bの代替サービス番号を利用した通信動作を説明するためのフロー図である。代替サービスを利用した通信では、まず、アプリケーションプログラムによる支援機能の利用可否を判断するため、システム稼動保証支援機構を利用することのできるアプリケーションが登録されているデータベース81の登録有無を確認する(ステップS1701)。登録されていればシステム稼動保証支援機構を利用可能であり、アプリケーションプログラムが通信したいサーバ91aとサービス名92aを探索し、探索結果に合致する該当行のサービス選択の選択値95aを取り出す(ステップS1702)。

【００４４】ここで選択値95aが「代替」である場合には、通信パケットの宛先サービス番号1002には該当行の代替サービス番号94aを設定し(ステップS1703)、送信する(ステップS1705)。

【００４５】一方、選択値95aが「既定」である場合には、通信パケットの宛先サービス番号1002には該当行の既定サービス番号93aを設定し(ステップS1704)、送信する(ステップS1705)。

【００４６】これに対し、システム稼動保証支援機構を利用することのできるアプリケーションがデータベース81に登録されていない場合には、通信パケットの宛先サービス番号1002には該当行の既定サービス番号93aを設定し(ステップS1704)、送信する(ステップS1705)。

【００４７】本実施例によれば、以下のような効果がある。

(1) システム稼動保証支援のサービス状態をコンピュータウイルスの拡散を抑止する状態に切替えた際には、事前に登録された正規のアプリケーションプログラムのみが代替サービス番号を使用して通信を行う。このため、コンピュータウイルスが代替サービス番号を使用して拡散することを抑止することができる。

【００４８】以下、本発明の第3実施例を図面によって説明する。第3実施例は、複数のシステム稼動保証支援装置31a，31cを多段にまたがり利用する場合の実施例である。

【００４９】図1のシステム稼動保証支援装置31の概略構成図、図2の電子計算機32の概略構成図、図10の通信用パケットのフォーマット、図5～図6のシステム稼動保証支援装置31a，31bで使用する通過サービスのアクセス制御情報に関するデータベース、図14～図15のコンピュータめのフロー図は、第1実施例と同じである。

【００５０】図4は、本実施例を適用したシステム稼動保証支援のネットワークシステム概略図である。システム稼動保証支援を行う装置31a，31c、そして、サーバ装置32c，32e、クライアント装置32dなどの電子計算機がネットワーク33b，33c，33dを介して接続している。

【００５１】図11に、システム稼動保証支援装置31cで使用する構成情報データベース134の一例を示す。図11は、システム稼動保証支援装置が多段に構成されている場合に、次に送信するシステム稼動保証支援装置を指定することのできるフィールドとして転送先サーバ1101，転送先サービス番号1102を追加した、サーバ毎にアプリケーションプログラムが使用するサービス番号とサービス選択状態の格納されたデータベースである。testserv2サーバ32eに対してサービス名httpに関わるトラフィックを利用してコンピュータウイルスが拡散している際の設定となっている。

【００５２】列91bにはサーバを一意に識別するネットワーク上の論理アドレス、列92bにはサーバアプリケーションプログラムのサービス名を一意に識別する名称、列93bには同じ行のサービス名がコンピュータウイルス拡散中ではない状態で使用するサービス番号、列94bには同じ行のサービス名がコンピュータウイルス拡散中に使用する代替サービス番号、列95bには同じ行のサービス名が使用するサービス選択状態が格納され、多段に構成されたシステム稼動保証支援装置を利用する際には、サービス選択状態として「転送」を格納する。

【００５３】testserv2サーバ32eに対してサービス名httpに関わるトラフィックを利用してコンピュータウイルスが拡散していることから、testserv2サーバ32eのサービス名httpではサービス選択状態値として「転送」、それ以外のサーバとサービス名ではサービス選択状態値として「既定」が格納される。列95bのサービス選択状態値として「転送」が格納されている場合には、列1101には同じ行のサービス名の通信を転送するサーバ、列1102には同じ行のサービス名の通信を転送するサービス番号が格納される。

【００５４】システム稼動保証支援装置として、31cから31aを経由するような多段構成の場合、クライアント装置32dでは、testserv2サーバ32eのサービス名httpについては宛先サーバ1001として「testserv2」、宛先サービス番号1002として代替サービス番号「9080」を設定した通信パケットを送信する。この通信パケットは、システム稼動保証支援装置31cにおいて、通信パケットの宛先アドレス1001に列1101の転送先サーバ「map1」を設定し、通信パケットの宛先サービス番号1002に列1102の転送先サービス番号「80」を設定した後、通信パケットのデータ部1005にクライアント装置32dが送信するオリジナルの通信パケットを格納するカプセル化形式とし

【００５５】ネットワーク2(33c)上の通信パケットは、宛先アドレス1001として転送先サーバ「map1」、宛先サービス番号1002として転送先サービス番号「80」が設定される。この通信パケットはさらに、システム稼動保証支援装置31aにおいて、通信パケットのカプセル化をほどき、オリジナルの通信パケットする。ネットワーク3(33d)上の通信パケットは、宛先サーバ1001として「testserv2」、宛先サービス番号1002として代替サービス番号「9080」を設定した通信パケットを送信する。しかし、コンピュータウイルスには構成変更情報を提供しないので、コンピュータウイルスはtestserv2サーバ32eのサービス名httpについては通信パケットの宛先アドレス1001として「testserv2」、宛先サービス番号1002として値「80」を使用し続けることになり、ネットワーク2(33c)上には送信されることはない。

【００５６】本実施例によれば、以下のような効果がある。

(1) システム稼動保証支援のサービス状態をコンピュータウイルスの拡散を抑止する状態に切替えた際には、ネットワーク2(33c)において、代替サービス番号に対するアクセス制御として「通過拒否」が設定されていた場合にも、コンピュータウイルスが使用する通信パケットを遮断し、かつ正規のアプリケーションプログラムの通信サービスを保証することができる。

【００５７】以下、本発明の第4実施例を図面によって説明する。第4実施例は、URLの書き換えにより代替サービスに切替えることができることを示す実施例である。

【００５８】図3のネットワークシステム概略図、図1のシステム稼動保証支援装置31の概略構成図、図2の電子計算機32の概略構成図、図10の通信用パケットのフォーマット、図5～図6のシステム稼動保証支援装置31a，31bで使用する通過サービスのアクセス制御情報に関するデータベース、図14～図15のコンピュータウイルス拡散時ならびに収束時の動作を説明するためのフロー図は、第1実施例と同じである。

【００５９】図12に、システム稼動保証支援装置31a，31bで使用する構成情報データベース134の一例を示す。図12は、サーバ毎のURL変換情報が格納されたデータベースであり、列1201aにはコンピュータウイルス拡散中ではない状態で使用する既定URL、列1202aには同じ行のURLがコンピュータウイルス拡散中に使用する代替URL、列1203aには同じ行のURLを転送するサーバ、列1204aには同じ行のURLを転送するサービス番号が格納される。

【００６０】testservサーバ32aに対してhttpに関わるトラフィックを利用してコンピュータウイルスが拡散している場合、クライアント装置32bでは、データ部1005に「http://testserv/」を設定した通信パケットをシステム稼動保証支援装置31aに送信する。この通信パケットは、システム稼動保証支援装置31aにおいて、通信パ

estserv」を格納し、通信パケットの宛先サービス番号1002に列1204aの転送先サービス番号「9080」を格納した後、データ部1005に「http://testserv:9080/」を格納を行い、testservサーバ装置32aに送信する。

【００６１】上記構成のシステム稼動保証支援装置31a，31bの動作について説明する。

【００６２】図18は、コンピュータウイルス拡散時のシステム稼動保証支援装置31aのURL書換えによる代替サービスを利用した通信動作を説明するためのフロー図である。代替サービスを利用した通信では、まず、データ部1005に「http://testserv/」を設定した通信パケットを受信すると、このURLをURL変換情報データベースの既定URL1201aから探索し(ステップS1801)、探索結果に合致する該当行の代替URL1202aを取り出した後、データ部1005に「http://testserv:9080/」を格納する(ステップS1802)。

【００６３】通信パケットの宛先アドレス1001には該当行の転送先サーバ「testserv」、宛先サービス番号1002には該当行の転送先サービス番号「9080」を設定し送信する(ステップS1803)。

【００６４】しかし、コンピュータウイルスには構成変更情報を提供しないので、コンピュータウイルスはtestservサーバ32aのサービス名httpについては通信パケットの宛先アドレス1001として「testserv」、宛先サービス番号1002として値「80」を使用し続けることになり、ネットワーク(33a)上には送信されることはない。

【００６５】本実施例によれば、以下のような効果がある。

(1) システム稼動保証支援のサービス状態をコンピュータウイルスの拡散を抑止する状態に切替えた際には、URLの書換えを行うため、アクセスするURLとサーバ装置32aが提供するサービス番号の不一致を回避できる。このため、コンピュータウイルスが使用する通信パケットを遮断し、かつ正規のアプリケーションプログラムの通信サービスにおいて、アクセスするURLのサービス上の不整合を排除することができる。

(2) システム稼動保証支援のサービス状態をコンピュータウイルスの拡散を抑止する状態に切替えた際にも、クライアント装置32bが利用するURLは、既存のURLを継続して利用することができるため、URLの変更を告知することなく、コンピュータウイルスが使用する通信パケットを遮断し、かつ正規のアプリケーションプログラムの通信サービスを継続して提供することができる。

【００６６】以下、本発明の第5実施例を図面によって説明する。第5実施例は、URLの書き換えにより代替サーバにより代替サービスを提供できることを示す実施例である。

【００６７】図4のネットワークシステム概略図、図1のシステム稼動保証支援装置31の概略構成図、図2の電子

マット、図5～図6のシステム稼動保証支援装置31a，31bで使用する通過サービスのアクセス制御情報に関するデータベース、図14～図15のコンピュータウイルス拡散時ならびに収束時の動作を説明するためのフロー図は、第2実施例と同じである。

【００６８】図13に、システム稼動保証支援装置31cで使用する構成情報データベース134の一例を示す。図13は、サーバ毎のURL変換情報が格納されたデータベースであり、列1201bにはコンピュータウイルス拡散中ではない状態で使用する既定URL、列1202bには同じ行のURLがコンピュータウイルス拡散中に使用する代替URL、列1203bには同じ行のURLを転送するサーバ、列1204bには同じ行のURLを転送するサービス番号が格納される。

【００６９】testserv2サーバ32eに対してhttpに関わるトラフィックを利用してコンピュータウイルスが拡散しており、ネットワーク2(33c)が高負荷トラフィック状況下にある場合、クライアント装置32dでは、データ部1005に「http://testserv2/」を設定した通信パケットをシステム稼動保証支援装置31cに送信する。この通信パケットは、システム稼動保証支援装置31cにおいて、通信パケットの宛先アドレス1001に列1203bの転送先サーバ「alt-testserv2」を格納し、通信パケットの宛先サービス番号1002に列1204bの転送先サービス番号「9080」を格納した後、データ部1005に「http://alt-testserv2:9080」を格納を行い、alt-testserv2サーバ装置32cに送信する。

【００７０】本実施例によれば、以下のような効果がある。

(1) システム稼動保証支援のサービス状態をコンピュータウイルスの拡散を抑止する状態に切替えた際には、URLの書換えにより、alt-testserv2代替サーバ32cに転送することができる。このため、本来のtestserv2サーバ32cに至るネットワーク33cが高負荷トラフィック状況下にあり性能を確保できない場合には、alt-testserv2代替サーバ32cに切替えることにより、性能を考慮したサービスを提供することができる。

(2) システム稼動保証支援のサービス状態をコンピュータウイルスの拡散を抑止する状態に切替えた際にも、クライアント装置32bが利用するURLは、既存のURLを継続して利用することができるため、URLの変更を告知することなく、コンピュータウイルスが使用する通信パケットを遮断し、かつ代替サーバによる正規のアプリケーションプログラムの通信サービスを継続して提供することができる。

【００７１】

【発明の効果】本発明によれば、コンピュータウイルスの駆除ツールが配布されていなくともコンピュータウイルスの拡散を抑止し、さらに、ネットワークシステムにおける正規のアプリケーションプログラムの通信を継続

【図面の簡単な説明】

【図１】システム稼動保証支援装置の概略構成図。

【図２】クライアント／サーバ装置の概略構成図。

【図３】実施例においてシステム稼動保証支援装置を適用したシステムの概略図。

【図４】実施例においてシステム稼動保証支援装置を適用したシステムの概略図。

【図５】通過サービスのアクセス制御情報が格納されたデータベースの一例。

【図６】通過サービスのアクセス制御情報が格納されたデータベースの一例。

【図７】サービス選択状態が格納されたデータベースの一例。

【図８】稼動支援サービス利用可能アプリケーションが登録されたデータベースの一例。

【図９】サーバ登録型のサービス選択状態が格納されたデータベースの一例。

【図１０】データパケットの一例。

【図１１】サービス転送型のサービス選択状態が格納されたデータベースの一例。

【図１２】ＵＲＬ変換情報が格納されたデータベースの一例。

【図１３】ＵＲＬ変換情報が格納されたデータベースの一例。

【図１４】システム稼動保証支援装置における支援機能の起動フローの一例。

【図１５】システム稼動保証支援装置における支援機能の回復フローの一例。

【図１６】クライアントにおける支援機能の起動フローの一例。

【図１７】クライアントにおけるアプリケーション登録型支援機能の起動フローの一例。

【図１８】システム稼動保証支援装置におけるＵＲＬ書き換えフローの一例。

【符号の説明】

S1401: システム稼動支援装置の切替え機構の判別ステップ

S1402: データパケット監視ステップ

S1403: データパケット監視による不正パケットの検出ステップ

S1404: 管理者による手動切り替えステップ

S1405: アクセス制御情報データベースの既定サービス番号を探索するステップ

S1406: 既定サービス番号に対するアクセス制御情報として"deny"を設定するステップ

S1407: 代替サービス番号に対するアクセス制御情報として"allow"を設定するステップ

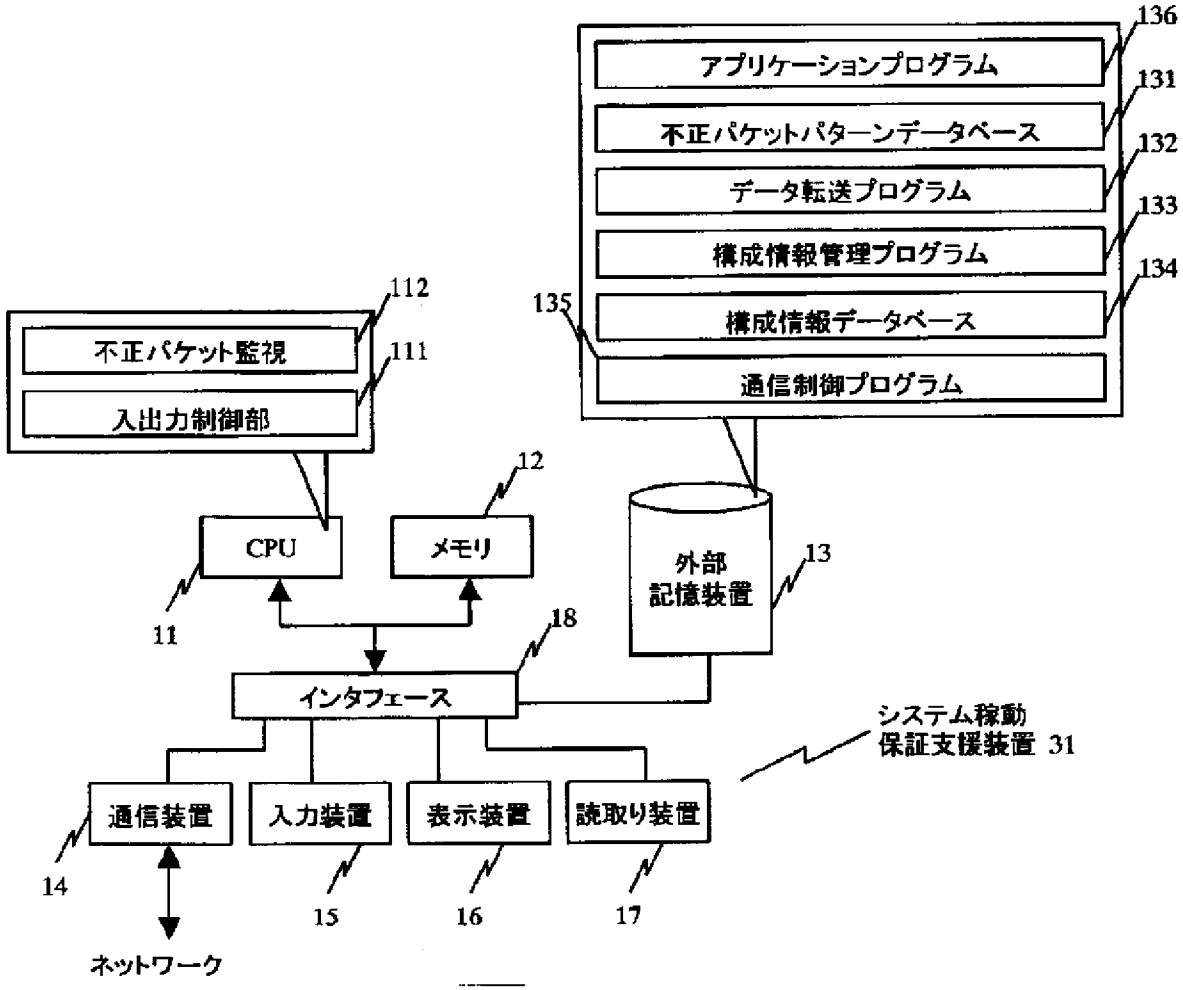
S1408: サービス選択状態データベースの既定サービス番号を探索するステップ

15 16

プ

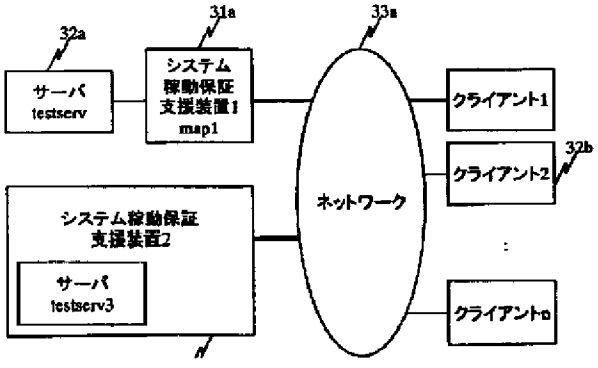
【図１】

図 1



【図３】

図 3



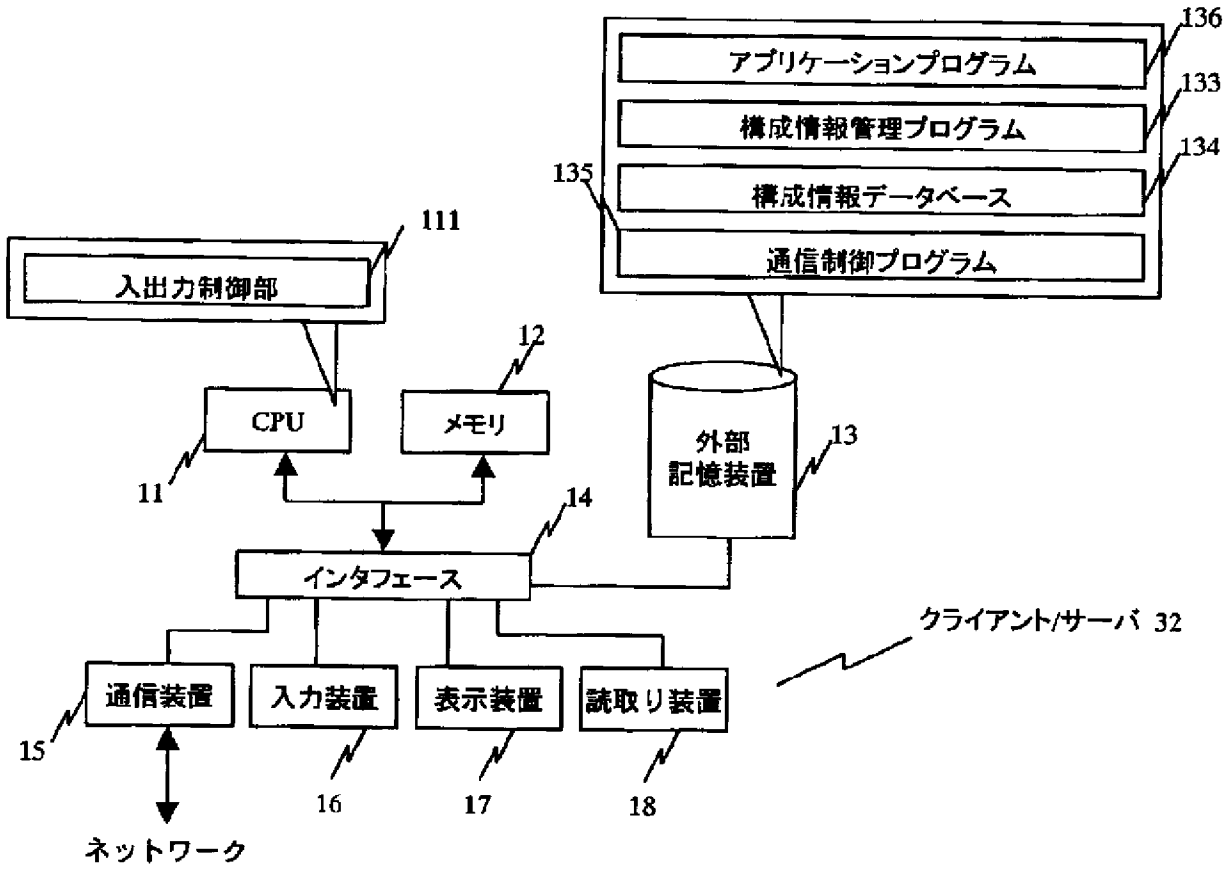
【図７】

図 7

71 サービス名	72 既定サービス番号	73 代替サービス番号	74 サービス選択
http	80	9080	代替
https	443	9443	既定
：	：	：	：

【図２】

図 2



【図５】

図 5

51a サービス名	52a 既定サービス番号	53a 通過可否	54a 代替サービス番号	55a 通過可否
smtp	25	allow	9025	deny
pop	110	allow	9110	deny
http	80	allow	9080	deny
https	443	allow	9443	deny
：	：	：	：	：

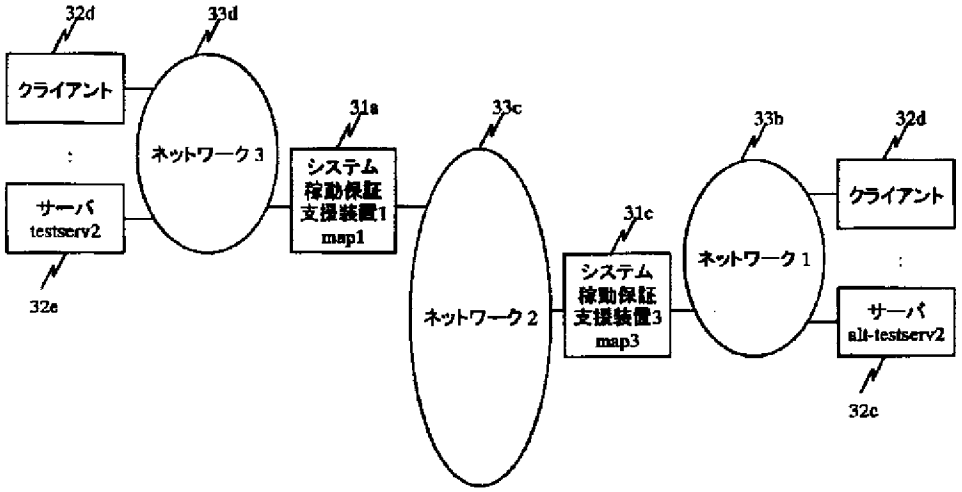
【図８】

図 8

81 アプリケーション名
webサーバプログラム websapp
メールサーバプログラム mailapp
webクライアントプログラム webbrowser
メールクライアントプログラム mailreader
：

【図４】

図 4



【図６】

図 6

51b サービス名	52b 既定サービス番号	53b 通過可否	54b 代替サービス番号	55b 通過可否
smtp	25	allow	9025	deny
pop	110	allow	9110	deny
http	80	deny	9080	allow
https	443	allow	9443	deny
:	:	:	:	:

【図９】

図 9

91a サーバ	92a サービス名	93a 既定サービス番号	94a 代替サービス番号	95a サービス選択
testserv	http	80	9080	代替
testserv	https	443	9443	既定
webserv	http	80	9080	既定
:	:	:	:	:

【図１０】

図 10

1001 宛先アドレス	1002 宛先サービス番号	1003 発信元アドレス	1004 発信元サービス番号	1005 データ
testserv	9080	クライアント1	555	abc

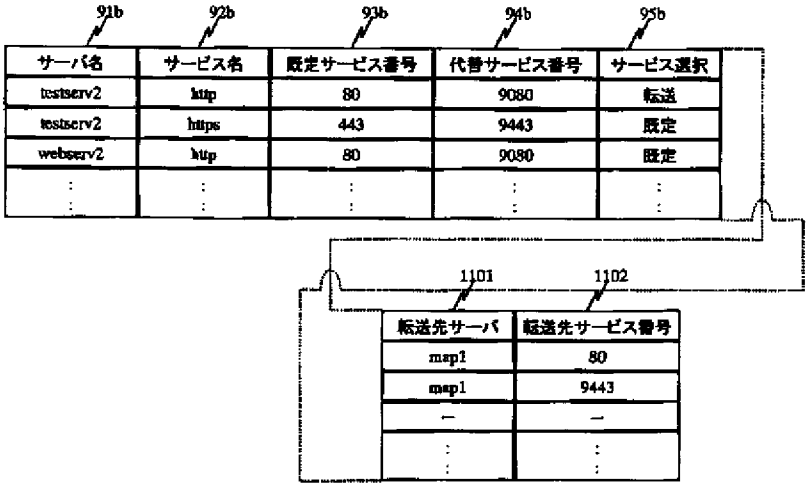
【図１２】

図 12

1201a 既定URL	1202a 代替URL	1203a 転送先サーバ	1204a 転送先サービス番号
http://testserv/	http://testserv:9080/	testserv	9080
https://testserv/	https://testserv:9443/	testserv	9443
:	:	:	:

【図１１】

図 11



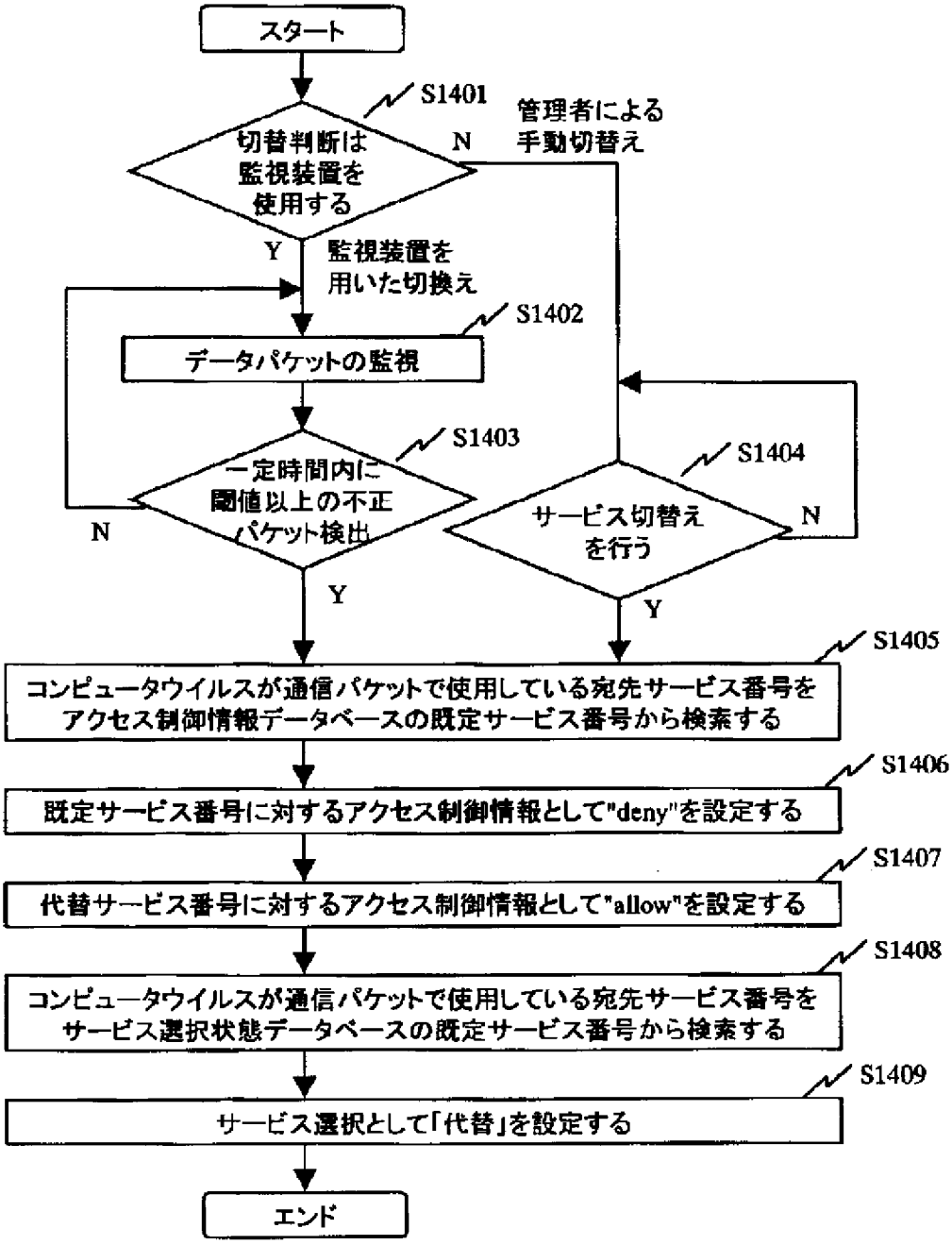
【図１３】

図 13

1201b 既定URL	1202b 代替URL	1203b 転送先サーバ	1204b 転送先サービス番号
http://testserv2/	http://alt-testserv2:9080/	alt-testserv2	9080
https://testserv2/	https://alt-testserv2:9443/	alt-testserv2	9443
:	:	:	:

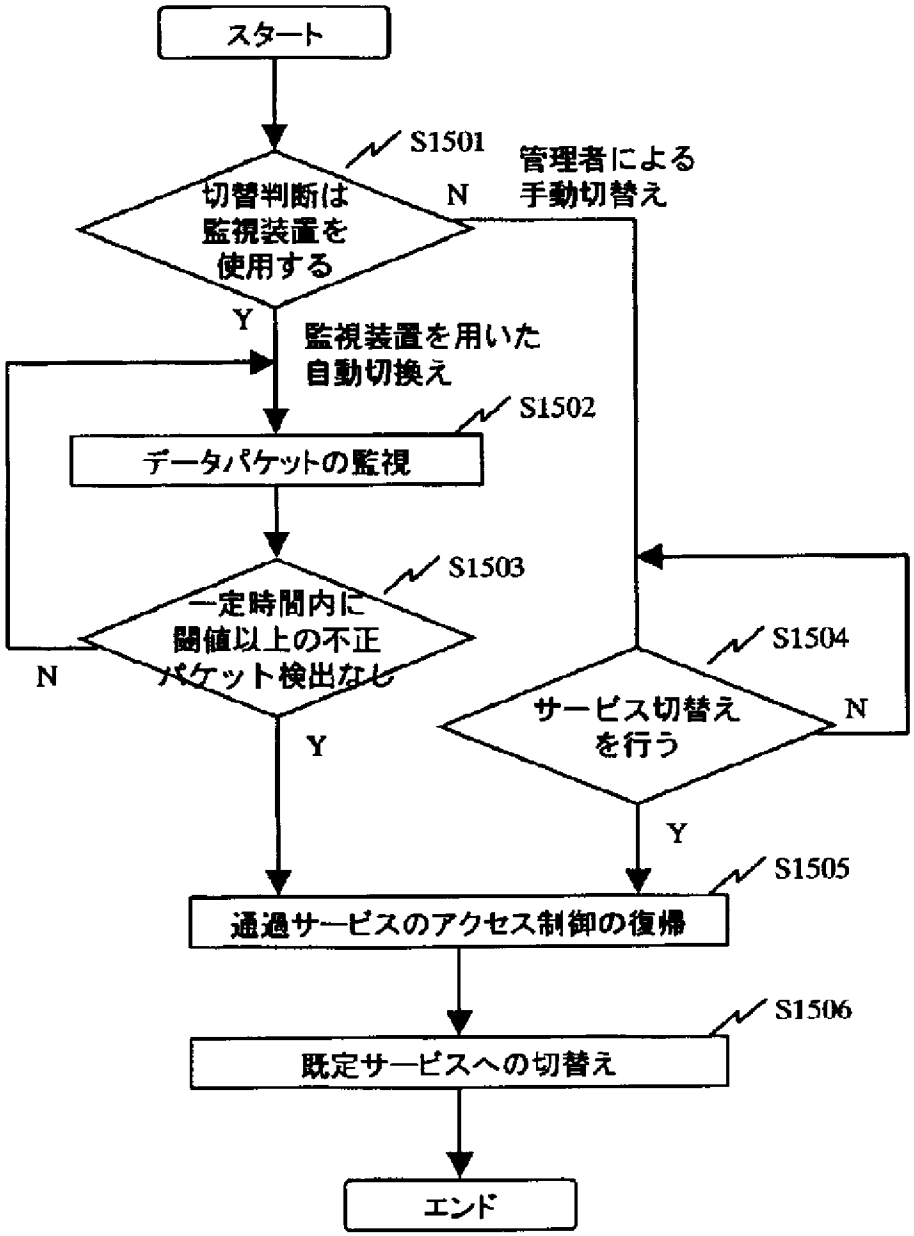
【図１４】

図 14


スタート
S1401
切替判断は監視装置を使用する
N
管理者による手動切替え
Y
監視装置を用いた切換え
S1402
データパケットの監視
S1403
一定時間内に閾値以上の不正パケット検出
N
Y
S1404
サービス切替えを行う
N
Y
S1405
コンピュータウイルスが通信パケットで使用している宛先サービス番号をアクセス制御情報データベースの既定サービス番号から検索する
S1406
既定サービス番号に対するアクセス制御情報として"deny"を設定する
S1407
代替サービス番号に対するアクセス制御情報として"allow"を設定する
S1408
コンピュータウイルスが通信パケットで使用している宛先サービス番号をサービス選択状態データベースの既定サービス番号から検索する
S1409
サービス選択として「代替」を設定する
エンド

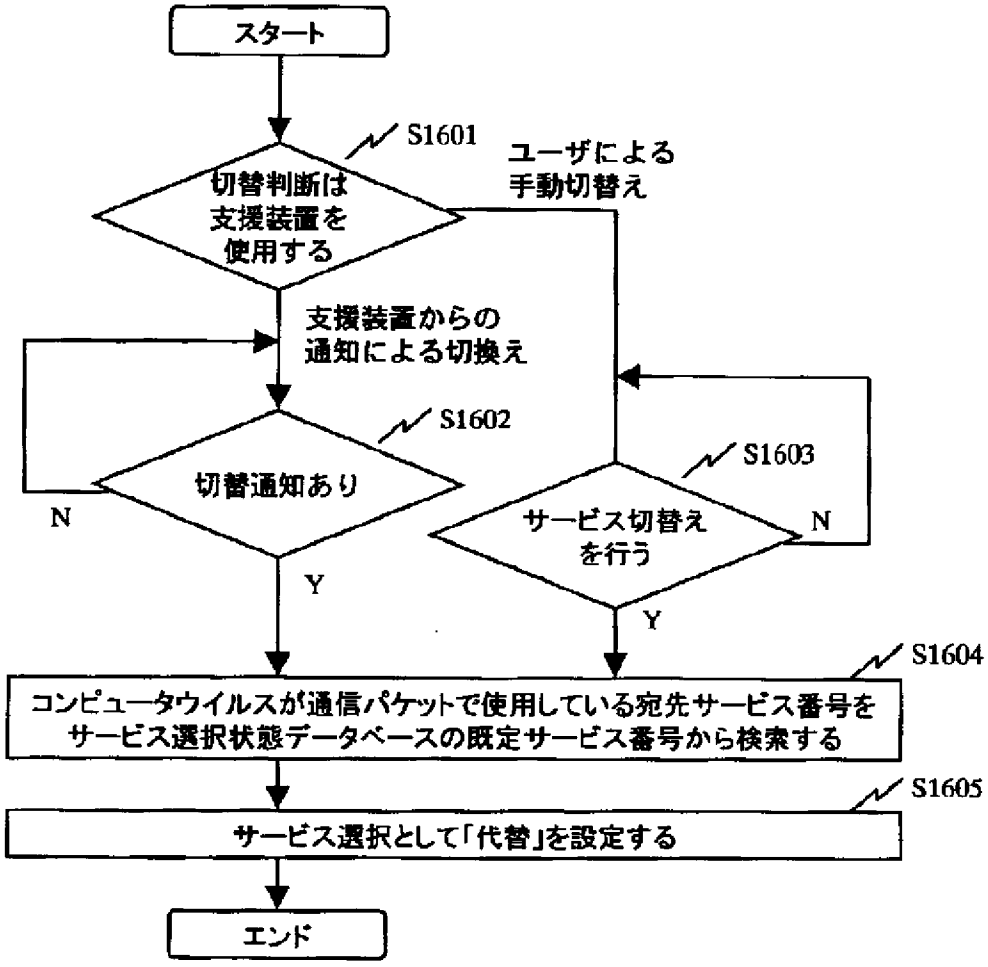
【図１５】

図 15


スタート
S1501
切替判断は監視装置を使用する
N
管理者による手動切替え
Y
監視装置を用いた自動切換え
S1502
データパケットの監視
S1503
一定時間内に閾値以上の不正パケット検出なし
N
Y
S1504
サービス切替えを行う
N
Y
S1505
通過サービスのアクセス制御の復帰
S1506
既定サービスへの切替え
エンド

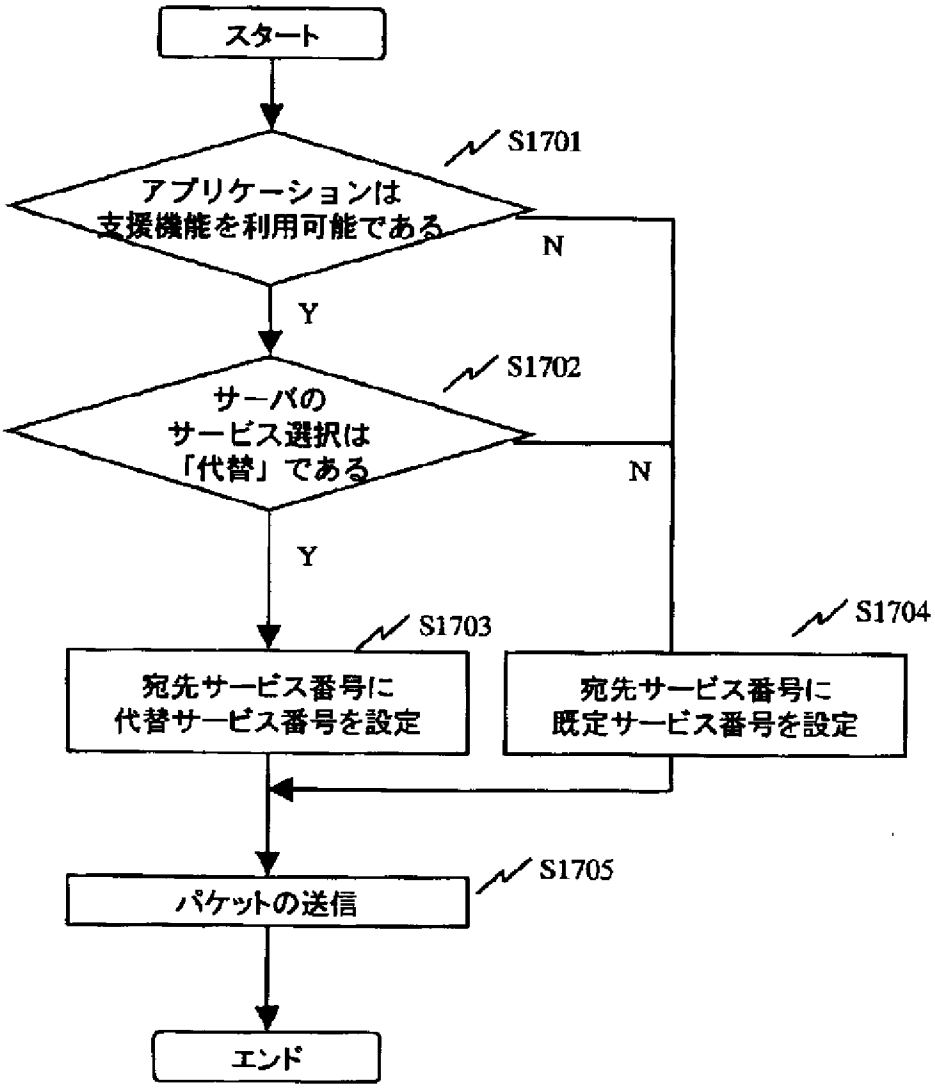
【図１６】

図 16


スタート
S1601
ユーザによる
手動切替え
切替判断は
支援装置を
使用する
支援装置からの
通知による切換え
S1602
切替通知あり
N
Y
S1603
サービス切替え
を行う
N
Y
S1604
コンピュータウイルスが通信パケットで使用している宛先サービス番号を
サービス選択状態データベースの既定サービス番号から検索する
S1605
サービス選択として「代替」を設定する
エンド

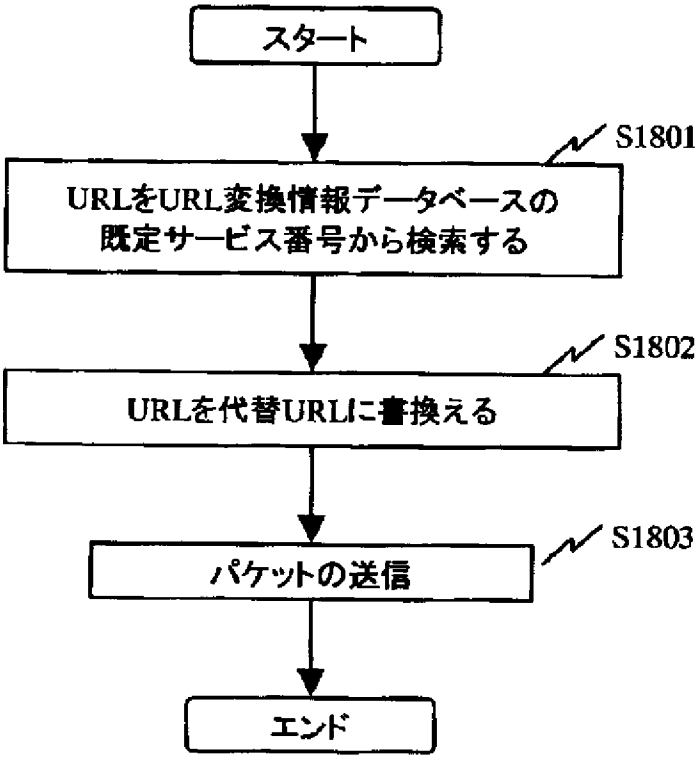
【図１７】

図 17


スタート
S1701
アプリケーションは
支援機能を利用可能である
N
Y
S1702
サーバの
サービス選択は
「代替」である
N
Y
S1703
宛先サービス番号に
代替サービス番号を設定
S1704
宛先サービス番号に
既定サービス番号を設定
S1705
パケットの送信
エンド

【図１８】

図 18



フロントページの続き

(72)発明者　長田　清人
神奈川県横浜市戸塚区戸塚町5030番地　株
式会社日立製作所ソフトウエア事業部内

Ｆターム(参考)　5B089 GA12 GA21 GB02 HA10 JB22
KA12
5K030 HC01 HD03 HD05 HD06